Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	**)**	
	)	
Digital Output Protection Technology	**)**	**MB Docket Nos. 04-55, 04-56,**
and Recording Method Certifications	**)**	**04-57, 04-58, 04-59, 04-60, 04-61,**
	)	**04-62, 04-63, 04-64, 04-65, 04-66,**
All Technologies and Recording Methods	**)**	**04-68**

PETITION FOR PARTIAL RECONSIDERATION AND CLARIFICATION BY THE MOTION PICTURE ASSOCIATION OF AMERICA, INC., METRO-GOLDWYN-MAYER STUDIOS INC., PARAMOUNT PICTURES CORPORATION, SONY PICTURES ENTERTAINMENT INC., TWENTIETH CENTURY FOX FILM CORPORATION, UNIVERSAL CITY STUDIOS LLLP, THE WALT DISNEY COMPANY, AND WARNER BROS. ENTERTAINMENT INC.

Jon A. Baumgarten
Bruce E. Boyden
Proskauer Rose LLP
1233 Twentieth Street NW, Suite 800
Washington, DC 20036
(202) 416-6800

September 13, 2004

TABLE OF CONTENTS

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	**)**	
	)	
Digital Output Protection Technology	**)**	**MB Docket Nos. 04-55, 04-56,**
and Recording Method Certifications	**)**	**04-57, 04-58, 04-59, 04-60, 04-61,**
	)	**04-62, 04-63, 04-64, 04-65, 04-66,**
All Technologies and Recording Methods	**)**	**04-68**

PETITION FOR PARTIAL RECONSIDERATION AND CLARIFICATION BY THE MOTION PICTURE ASSOCIATION OF AMERICA, INC., METRO-GOLDWYN-MAYER STUDIOS INC., PARAMOUNT PICTURES CORPORATION, SONY PICTURES ENTERTAINMENT INC., TWENTIETH CENTURY FOX FILM CORPORATION, UNIVERSAL CITY STUDIOS LLLP, THE WALT DISNEY COMPANY, AND WARNER BROS. ENTERTAINMENT INC.

The Motion Picture Association of America, Inc. ("MPAA"), Metro-Goldwyn-Mayer Studios Inc., Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLLP, The Walt Disney Company, and Warner Bros. Entertainment Inc. (collectively, "the MPAA Parties") hereby submit this petition for partial reconsideration and clarification of the Commission's August 4, 2004 Order (the "Certification Order").[1]

INTRODUCTION AND SUMMARY

As certified, eleven of the thirteen technologies approved by the Commission adequately protect digital broadcast television programming, and we applaud the Commission's actions in quickly approving their certifications so as to move the digital transition forward on an expedited

[1] Order, *Digital Output Protection Technology and Recording Method Certifications*, MB Docket Nos. 04-55, *et al.*, FCC 04-193 (rel. Aug. 12, 2004).

basis. However, we believe that the Certification Order should be reconsidered in three respects. First, the Commission's decision to approve TiVo's certification for TiVoGuard and the Smart-Right Group's certification for SmartRight without conditioning those approvals on incorporation of proximity controls is in error, and the Certification Order should be amended to require proximity controls in both such technologies.[2] Second, the Commission should expressly prohibit the use of mixed networks comprised of both affinity-based and proximity-based technologies until "daisy chains" resulting in indiscriminate redistribution can be prevented when content is transferred between technologies. Finally, the Commission should reconsider its decision to require preliminary approval of material changes where effective change management procedures are provided in a private content participant agreement.

I. The Commission Should Reconsider Its Authorization of TiVoGuard for Use With the Broadcast Flag and Should Clarify That SmartRight Is Authorized Only With the Inclusion of Proximity Controls

A. Authorization of Remote Access Capability for TiVoGuard and SmartRight in the Interim Certification Process Was Premature

We believe the Commission erred in determining that "we are not inclined as part of our review of these certifications to impose proximity controls as an additional obligation where other reasonable constraints sufficiently limit the redistribution of content."[3] The Commission's decision to authorize remote access capability in proposed technologies is premature at this time for two reasons. First, the Commission's Certification Order undermined the Commission's own

[2] Thomson has announced that SmartRight will incorporate proximity controls. *See* Paul Gluckman, *Thomson Reaffirms Pledge to Impose SmartRight Proximity Controls*, Consumer Electronics Daily, Aug. 30, 2004. So long as Thomson abides by this promise, the MPAA Parties request with respect to SmartRight only that the Commission reverse the precedent that may be set by its decision. For the record, we do not believe that the Certification Order binds the Commission to approving similar technologies in the future, as the Commission itself has recognized. *See* Certification Order ¶ 73 ("[D]eterminations of whether proximity controls are necessary or desirable must be made on a case-by-case basis . . . .").

[3] Certification Order ¶ 72.

notice and comment rulemaking. Other proceedings are also currently underway on issues that will help resolve the very questions raised by the TiVoGuard certification, such as the proper criteria for remote access. The Commission therefore should require proximity control for now, permitting remote access capability only for defined technologies submitted *after* the criteria necessary to allow secure remote access have been devised and commented upon by the interested parties in the pending rulemaking.

Second, the Commission's authorization of remote access capability is particularly premature as regards TiVoGuard. TiVoGuard is a nascent technology that is exceedingly ill-defined and that even TiVo now admits is "still at the concept stage."[4] TiVo has stated to the press that "the company has not yet designed a DVR capable of using" remote access functionality, "nor is there a timetable for the product."[5] Given the lack of specificity in TiVoGuard's design (particularly with respect to how TiVoGuard would effectuate remote access), the Commission had no reason not to condition authorization of TiVoGuard on inclusion of proximity controls until the many complicated issues surrounding remote access are resolved.

In addition, TiVoGuard's lack of definition resulted in a number of vague, conclusory, and sometimes inconsistent statements in the record concerning its capabilities that prevented adequate Commission review and hampered content owners' ability to comment on the technology. For example, TiVo failed to supply a copy of its proposed end-user license agreement which TiVo claimed prohibited unauthorized redistribution. Furthermore, considerable uncertainty remains as to how the technology will operate, such as the maximum

[4] Robin Arnfield, *FCC Certifies TiVo Internet Technology*, NewsFactor, Aug. 4, 2004 (attached as Exhibit A). This article is "evidence which has become available only since the original taking of evidence," 47 C.F.R. § 1.106(l), and is thus properly considered on reconsideration.

[5] Jonathan Sidener, *TiVo Owners Could Share Shows Online*, San Diego Union-Tribune, Aug. 5, 2004 (attached as Exhibit B).

number of devices that would be permitted in a so-called "Secure Viewing Group" ("SVG"), and the process for granting certain users additional devices beyond the maximum number.

TiVo has also been vague about important aspects of the relationship between TiVo subscribers and the handling of protected DTV content by TiVoGuard. TiVo claimed that "TiVoGuard limits the redistribution of protected content to a secure viewing group of devices that belong to the same owner and that are associated with the same TiVo service account, which must in turn be billed to the owner's credit card."[6] But TiVo has never stated that it has any means whatsoever of ensuring that the devices in an SVG must "belong to the same owner,"[7] and the Commission's reliance on this point was therefore misplaced. Nor has TiVo ever provided details concerning the constraints it would impose, if any, to prevent rapid, successive re-registration of a device in different SVGs. Without time constraints on re-registration, a device could be re-registered in rapid succession into different SVGs, providing that device to move content from one SVG to another without physically moving the device.

TiVo similarly conflated the difference between a TiVo service subscription, on the one hand, and registration of a particular TiVoGuard device with an SVG, on the other. Although the record is far from clear, a TiVo *subscription* apparently allows a device to receive the TiVo menu and channel guide. TiVo service subscriptions must be purchased using a credit card. *Registration of a device*, on the other hand, is the process by which TiVo boxes and TiVoToGo dongles are identified as belonging to the same SVG. Many key facts concerning registration of a TiVo device are absent from the record. For example, insofar as it can be determined from TiVo's Certification, TiVo does not require a user of a TiVo device to enter his or her credit card

[6] Certification Order ¶ 20.

[7] Certification Order ¶ 20.

number to register a device or dongle in an SVG, nor does TiVo require every device and dongle registered in an SVG to have a TiVo subscription. Further, despite what TiVo originally claimed,[8] TiVo does not require all TiVo devices with subscriptions to be paid for using the same credit card. Indeed, TiVo has admitted that its prior assertion that all TiVo devices in an SVG must be registered to one credit card is incorrect.[9]

The record before the Commission therefore fails to indicate that TiVo has any means to ensure that content sent over TiVoGuard is indeed sent to devices belonging to, or even associated with, a single subscriber. It appears that the device registration process may consist of nothing more than typing a serial number into a website. Once registered in a person's SVG in this manner, TiVo apparently has no way of tracking the location of the dongles and devices in an SVG or who is using them. Such lapses invite foreseeable mischief. A sports bar may pay TiVo subscribers in other markets to register the sports bar's devices in the subscribers' markets; or, individuals may sell their registered dongles on eBay so that others may receive distant signals. These lacunae in the record are critical in evaluating whether TiVoGuard affords sufficient protection to digital broadcast content.

While it is not necessary for a technology to have entered the marketplace to be submitted for Commission approval, the Commission should evaluate and approve only well defined technologies. Vague promises and speculations about the capabilities of a technology may be difficult or impossible to enforce after the technology is approved, and therefore, premature approval of such ill-defined technologies may threaten the Flag regulation. It was impossible for content owners to fully evaluate TiVoGuard, and unreasonable for the

[8] See Letter from James M. Burger to Susan Mort, June 22, 2004, Attachment at 3 ("TiVo White Paper").

[9] *See* Letter from James M. Burger to Marlene H. Dortch, July 21, 2004, Attachment at 2 n.1 ("TiVo does not require credit cards to be the same.").

Commission to have approved it, on the basis of mere design concepts. TiVoGuard should not be approved until its usefulness and potential for abuse are better described and understood than is possible today.

B. Without Proximity Controls, TiVoGuard and SmartRight Do Not Prevent Indiscriminate Redistribution of Broadcast Content

The Commission found in its November 4, 2003 Report & Order (the "Broadcast Flag Order")[10] that "content owners are justifiably concerned about protecting all DTV broadcast content, including both standard definition and high definition formats, from indiscriminate retransmission in the future."[11] The Commission concluded that in order to "ensure the continued availability of high value DTV content to consumers through broadcast outlets," DTV devices "must have some mechanism for protecting digital broadcast content."[12] The Commission decided that protection against "indiscriminate redistribution" would be adequate to achieve this goal.[13]

In the Certification Order, the Commission erroneously decided, on the basis of an inadequate record as detailed above, that "TiVoGuard . . . meet[s] the Commission's stated goal of preventing indiscriminate redistribution."[14] The Commission stated two reasons for this conclusion: first, the Commission pointed to restrictions contained in TiVo's subscriber agreement; second, the Commission stated that "[t]he limit of 10 devices uniquely associated with a single secure viewing group additionally prevents content from being redistributed in a

[10] Report and Order and Further Notice of Proposed Rulemaking, *Digital Broadcast Content Protection*, MB Docket No. 02-230 (rel. Nov. 4, 2003).

[11] *Id.* ¶ 8.

[12] *Id.*

[13] *Id.* ¶ 10.

[14] Certification Order ¶ 72.

'daisy chain' fashion."[15] In addition to these two explicit reasons, the Certification Order also cited other claims made by TiVo that may have influenced the Commission's decision. As demonstrated below, however, the Commission's two stated reasons do not support its conclusion, and the other claims made by TiVo are erroneous. The Commission should therefore reconsider its decision not to require proximity controls in TiVoGuard and should instead require them.

The Commission's first stated reason, that TiVo's user agreement prohibits infringement, is irrelevant and fails to support the Commission's conclusion. The goal of the Broadcast Flag regulation was to advance the digital transition by protecting digital broadcast content through *technological measures.*[16] While admittedly useful and even necessary in enforcing compliance by users with technological protection measures, a user agreement is not itself a technological protection measure, and TiVo never introduced any evidence that it can technologically enforce its subscriber agreement in any way.[17] Accepting a user agreement as a substitute for a technological protection measure is a dangerous precedent.

The Commission's second stated reason for its approval of TiVoGuard without proximity controls was that TiVoGuard purportedly does not permit broadcast content to be "redistributed

---

[15] *Id*. The conditions under which SVGs may be expanded to 20 devices remain unclear. The Commission in the Certification Order, ¶ 20 n.78, states that "[w]ritten waiver requests must indicate: (1) why a waiver is necessary, (2) where the devices will be located, (3) that the subscriber reaffirms the provisions in the TiVo user agreement requiring the subscriber not to violate copyright laws and pledging to only use copyrighted content for personal, non-commercial purposes. TiVo indicates that it will exercise care and consistency in granting waivers. Waivers may be granted for up to 20 devices, although the current technical limit is 16." (Citations omitted.) The Commission cites a July 28, 2004 *ex parte* from TiVo and the TiVoGuard Certification for this information; however, neither document contains these statements.

[16] Broadcast Flag Order ¶ 8 ("In order to effectively address [piracy] concerns, . . . we believe that *technological steps* must be taken . . . .") (emphasis added); *id.* ¶ 9 ("The creation of a redistribution control regime establishes a *technical protection measure* that broadcasters may use to protect content.") (emphasis added).

[17] *See* E-Mail from Bruce Boyden to Stacy Fuller, July 21, 2004, *attached to* Letter from Bruce E. Boyden to Marlene H. Dortch, July 21, 2004; *see also* MPAA White Paper at 9 (TiVo has no means of knowing of violations, and will likely not define violations adequately).

in a 'daisy chain' fashion,"[18] where Person A sends the content to Person B, who in turn sends the content to Person C. This reason too, however, is insufficient to support authorization of TiVoGuard. Daisy-chain redistribution is not the only threat posed by inadequate content protection technologies. For example, even when content is kept within a so-called "Secure Viewing Group," TiVoGuard facilitates widespread and simple redistribution of broadcast content between total strangers without any transfer of a physical object between them. All that may be required is that Person B provide Person A with his or her TiVo device's (or TiVoToGo dongle's) serial number. Person A can then register the device or dongle in his or her SVG, without paying any additional fee, and Person B will have unfettered access to Person A's library of recorded programs, as well as real-time access to all of Person A's future programs.[19]

In addition, the record does not support the Commission's conclusion that TiVoGuard does not enable "daisy-chain" redistribution. TiVo introduced no evidence concerning what constraints, if any, it places on users' ability to move devices and dongles between SVGs. If devices and dongles can be easily switched back and forth between SVGs, TiVoGuard would enable "daisy-chain" redistribution. The TiVoGuard system would also allow "daisy-chaining" by means of a physical dongle exchange. Person A could use TiVoGuard to send content easily to Person B, a total stranger whose TiVoToGo dongle is registered in Person A's SVG. Person B could then send all of their programs to Person C using a simple FTP transfer, and then share their TiVoToGo dongle with Person C, who would then have access to all of Person A's out-of-market programs.

---

[18] Certification Order ¶ 72.

[19] To the extent that Person B then wants to transfer all of those recorded programs, and all future programs, to Person C, all that will be required is a one-time physical transfer of the dongle or device, which as we have argued previously, places TiVoGuard in a much different realm than physical media, which requires an investment of time, materials, and postage for *each program* a person wishes to send. *See* Letter from Bruce E. Boyden to Marlene H. Dortch, July 16, 2004, Attachment at 4 ("MPAA White Paper").

Many of these same concerns apply to SmartRight as well, absent the inclusion of proximity controls. The Commission concluded, erroneously, that SmartRight met "the Commission's stated goal of preventing indiscriminate redistribution" through its use of a "smart card-based PPN structure and associated cap of 10 display devices."[20] Without proximity controls, however, nothing prevents each SmartRight Personal Private Network ("PPN") from being used to indiscriminately redistribute broadcast television content to up to nine total strangers. SmartRight's PPN is in this regard no different from TiVo's SVG.

The reasons proffered by the Commission therefore do not support its conclusions and are inconsistent with its stated goal of preventing indiscriminate redistribution. Furthermore, the Commission entirely failed to consider an important factor in weighing the harm to broadcast programming posed by use of TiVoGuard and SmartRight without proximity controls: namely, the adverse consequences of the Commission's failure to require proximity controls by TiVoGuard and SmartRight are greatly magnified when not just one SVG or PPN is considered, but the entire universe of future TiVo and SmartRight devices, and multiplied further upon consideration of the universe of all other future devices with similar functionality that may hereafter gain Commission approval on the precedential basis of TiVo's and SmartRight's certifications.[21] When this future universe is considered, it is plain that TiVoGuard and SmartRight, as certified by the Commission, will enable unrestrained, indiscriminate redistribution of digital broadcast content. The Commission therefore erred in concluding that TiVoGuard and SmartRight do not need proximity control because they contain "other

[20] Certification Order ¶ 72.

[21] Obviously, not all TiVoGuard devices will be used for redistribution. But it is also true that many consumers would not redistribute content even if their devices contained no protection at all. The point is that the harm to broadcast television stemming from inadequate protection that the Commission should evaluate is the collective harm that occurs nationwide, not just that resulting from an individual user's actions.

reasonable constraints [that] sufficiently limit the redistribution of content."[22] Indeed, the basis on which the Commission decided that TiVoGuard's and SmartRight's affinity-based controls were sufficiently protective of broadcast television content is opaque. Rather than evaluate the amount of redistribution enabled by each, the Commission stated only that TiVoGuard and SmartRight "meet the Commission's . . . goal."[23]

To the extent that the Commission relied on other factual statements and arguments by TiVo summarized in the Certification Order, many of those are in error or inapposite and therefore fail to support the Commission's decision. For example, TiVo argued that "technical limits" prevent TiVo users from sending real-time or even recorded programs to each other over the Internet.[24] This argument is entirely inconsistent with the Commission's earlier conclusion that "we anticipate that the potential for piracy will increase as technology advances,"[25] which justified the adoption of the Flag regulation in the first place. Indeed, the evidence continues to accumulate that current trends are rapidly increasing the speed and ease with which audiovisual content can be redistributed.[26] Content protection technology providers therefore cannot complacently rely on narrow bandwidth and large file sizes if the Broadcast Flag regulation is to be effective.

---

[22] Certification Order ¶ 72.

[23] *Id.*

[24] Certification Order ¶ 72 & n.321.

[25] Broadcast Flag Order ¶ 8.

[26] *See* Bernhard Warner, *Livewire: Beep! Beep! Ultra-Fast Broadband Is Here*, Reuters, Aug. 28, 2004 (10 and 100 mbps broadband now available to consumers in Sweden) (attached as Exhibit C); *see also* Lee Gomes, *Coming Soon: Movies You Rent on the Web – and Then Download*, Wall St. J., Aug. 30, 2004, at B1 ("In these days of increasing broadband speeds and gargantuan disk drives, time and size are no longer major problems.") (attached as Exhibit D).

TiVo's claims concerning revocation and renewal are similarly unreliable. For example, the Commission concluded that revocation and renewal issues could be resolved due to TiVo's "continued collaboration" with content owners.[27] While TiVo has met with content owners to discuss our concerns with TiVoGuard – something we applaud – such meetings have not resulted in any concrete steps by TiVo to address those concerns and certainly do not rise to the level of "continued collaboration." Nor does TiVoGuard "currently [have] in place appropriate mechanisms to disseminate revocation and renewal information."[28]

Given the state of the record and the concerns noted above, the Certification Order fails to adequately explain the reasons for authorizing TiVoGuard and SmartRight without inclusion of proximity controls. Moreover, the Commission's decision is inconsistent with the Commission's stated goal of preserving the viability of over-the-air broadcast television. As the MPAA Parties argued in response to the TiVoGuard and SmartRight applications for certification, the broadcasting business in the United States is based on the notion of proximity control, in the form of a television station's transmitter footprint. Syndication, program licensing, local advertising, and sports blackouts are all premised on broadcast television programming being limited to a particular geographic area.[29] The Commission has recognized the importance of proximity control in the past in addressing distant signals and syndicated exclusivity. In approving technologies to redistribute content based on hypothetical restrictions, the Commission has unnecessarily undertaken a serious risk that may threaten the viability of the very broadcast system the Commission is endeavoring to protect.

[27] Certification Order ¶ 101.

[28] *Id.* ¶ 103.

[29] MPAA White Paper at 5-6.

C. The Commission Should Retain Oversight of Any Mixture of "Affinity-Based" and "Proximity-Based" Technologies to Ensure That Content Protection Is Not Evaded

The Commission has approved some technologies, such as DTCP, WMDRM, and Helix that rely on proximity-based controls, and others such as TiVoGuard that purportedly rely on affinity-based controls. The Commission has noted TiVo's plan to possibly mix the two types of technologies together by permitting TiVo devices to output decrypted TiVoGuard content from an SVG over "another Commission-approved output protection technology."[30] However, the mixture of the two types of controls can be used to subvert both proximity-based controls and affinity-based controls. By alternating the use of the two types of controls, restrictions on redistribution can be evaded and a "daisy chain" of redistribution created, first by using an affinity-based network to transmit content to a new location, then using a proximity-based technology to connect to a device on a network associated with another person, then using an affinity-based network again. For example, suppose someone uses TiVoGuard to send content to their vacation home, to a device within the sending device's SVG. If the vacation home TiVo has a DTCP output, that output could be used to send content to another TiVo in the vacation home belonging to a different SVG. The content could then be sent across the country again, then across another DTCP output to a third SVG, and so on, ad infinitum. The Commission should therefore not approve such mixed uses of affinity-based and proximity-based controls unless the technology proponent has specified how it intends to maintain the relevant limits when content is transferred between the different approved technologies.

TiVo has not proposed how it intends to keep content within SVGs even after output over technologies such as DTCP or WMDRM; therefore, TiVoGuard should not be allowed to link to

[30] Certification Order ¶ 22.

other Commission-approved technologies until TiVo provides specific measures to maintain the relevant content controls for each Commission-approved technology it seeks to use.

II. The Commission Should Reconsider Its Decision to Require Authorized Digital Output Protection Technologies or Recording Methods With Content Participant Agreements to Submit Material Changes for Prior Approval

In the Certification Order, the Commission wisely decided not to "grant blanket approvals under which a technology proponent could subsequently make material and substantial changes to their technology or license terms."[31] The MPAA Parties applaud the Commission for taking an active role in ensuring that its goals are not subverted by post-approval changes to the technologies. The Commission was right to require prior approval of material changes to those technologies whose proponents have not provided a content participant agreement with effective change management procedures.

However, as the Commission itself recognizes, it is properly "reluctant to intervene in private industry negotiations."[32] As it has done in similar contexts,[33] the Commission should therefore refrain from requiring prior Commission approval of changes to a technology or its license where privately negotiated content participant agreements contain effective change management provisions.[34] Such prior approval is particularly inappropriate when, as here, negotiated change management procedures that protect the interests of all parties, including providers of digital broadcast television content, already have been subject to review and

[31] Certification Order ¶ 98.

[32] *Id.* ¶ 80.

[33] See below.

[34] "Effective change management" means change management that gives content owners a meaningful opportunity to object to changes that may harm the security of the technology or security-related license terms, including an opportunity to arbitrate any disputes before a neutral third party. For licensed technologies, third-party adopters also benefit from reasonable change management provisions. Examples of effective change management provisions include those in the licenses for DTCP, HDCP, CPRM, D-VHS and Vidi/VCPS.

approval by the Commission. An additional layer of required regulatory review with respect to particular agreed changes flowing from the approved change management process is superfluous and will only delay the development and implementation of needed or useful improvements to existing and future certified technologies.

Furthermore, since some technologies may be used in other distribution channels and material changes may be proposed with respect to handling content in those channels, a requirement of prior Commission approval of such changes would be inconsistent with the Commission's determination that no "aggrandizement" of the Commission's decision occur through extension to other contexts. The role the Commission has created for itself in the change management process therefore is both a departure from prior practice and from the Commission's statements in this proceeding, and the record does not support the Commission's action in this respect.

In general, in the Certification Order, the Commission allowed private negotiations and license agreements to govern the technologies, maintaining only a general oversight role to resolve any disputes. The Commission thus declined to take control of downstream technology approvals, particular technology licensing terms, enforcement of adopter licenses, and revocation and renewal.[35] There is no distinction in the record or in the Certification Order between those situations and change management. Where effective change management procedures exist in a private content participant agreement, therefore, the Commission should allow them to operate without the need for prior Commission approval.

Layering a Commission approval mechanism on top of effective private change management procedures also is contrary to Commission precedent. We are unaware of any

[35] *See* Certification Order ¶¶ 83, 91, 93, 101.

instance in which the Commission has supplanted a collaboratively designed, fully functioning change management mechanism. Indeed, the only instance in which the Commission has ever even reviewed privately negotiated change management processes appears to have been in the telecommunications context, where the Commission has been required to do so by the Communications Act of 1996, which directs the Commission to review and approve the change management processes developed by the Bell Operating Companies ("BOC") for use with their operations support systems as part of their market-opening obligations.[36] The Commission has done so on over twenty occasions but has never substituted its own approval mechanism for that of a functioning BOC change management process.[37] The Commission also has ordered merging BOCs to rationalize and streamline their existing change management processes, but in doing so the Commission has neither dictated the terms of those plans nor replaced those terms with its own.[38] Only when disputes have arisen between a BOC and a new entrant has the Commission interceded – and then only to resolve administrative matters or to determine whether the BOC is meeting the requirements of the negotiated change management process.

For all of these reasons, the Commission should reconsider its decision to require pre-approval of material changes where effective private change management provisions exist in a private content participant agreement.

---

[36] *See* 47 U.S.C. §§ 251, 271; *see also In re Local Competition Provisions in the Telecommunications Act of 1996*, 11 FCC Rcd 15499, 15766 (¶ 523) (1996) (citations omitted).

[37] *See, e.g., In the Matter of Application by Qwest Communications Int'l Inc.*, 18 FCC Rcd ¶¶ 20-25 (2003); *In the Matter of Application by Qwest Communications Int'l Inc.*, 18 FCC Rcd 13,323 ¶¶ 134-40 (2003); *In the Matter of Application by SBC Communications Inc.*, 18 FCC Rcd 19,024 ¶¶ 117-26 (2003).

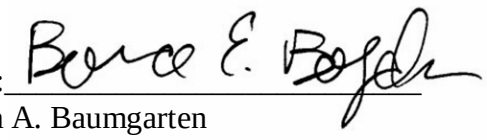
[38] *See, e.g., In re Applications of Ameritech Corp. and SBC Communications Inc.*, 14 FCC Rcd 14,712 ¶ 382 (1999).

CONCLUSION

For the reasons stated above, the certifications approved by the Commission should be reconsidered in part and clarified to require proximity controls in TiVoGuard and SmartRight, respectively; the Commission should clarify that mixed networks comprised of both affinity-based and proximity-based technologies must contain adequate controls; and the Commission should reconsider its decision to require prior approval of material changes even where effective change management procedures are provided in a private content participant agreement.

Respectfully submitted,

THE MOTION PICTURE ASSOCIATION OF AMERICA, INC.
METRO-GOLDWYN-MAYER STUDIOS INC.
PARAMOUNT PICTURES CORPORATION
SONY PICTURES ENTERTAINMENT INC.
TWENTIETH CENTURY FOX FILM CORPORATION
UNIVERSAL CITY STUDIOS LLLP
THE WALT DISNEY COMPANY
WARNER BROS. ENTERTAINMENT INC.

By: 

Jon A. Baumgarten
Bruce E. Boyden
Proskauer Rose LLP
1233 Twentieth Street NW, Suite 800
Washington, DC 20036
(202) 416-6800

Counsel for the Petitioners

CERTIFICATE OF SERVICE

I, Bruce E. Boyden, hereby certify that a true and correct copy of the Petition for Partial Reconsideration and Clarification by the Motion Picture Association of America, Inc., et al., was served on the following parties on September 13, 2004, by first-class mail, postage prepaid:

Jonathan L. Rubin, P.A.
1717 K Street NW, Suite 600
Washington, DC 20036
Counsel for American Antitrust Institute

Christopher Murray
Consumers Union
1666 Connecticut Ave. NW
Washington, DC 20009
Counsel for Consumers Union

Seth D. Greenstein
McDermott, Will & Emery
600 Thirteenth St. NW
Washington, DC 20005-3096
Counsel for Digital Transmission Licensing Administrator LLC

Bruce H. Turnbull
Weil, Gotshal & Manges LLP
1501 K Street NW, Suite 100
Washington, DC 20005
Counsel for 4C Entity LLC, Digital Content Protection LLC, and Victor Co. of Japan Ltd.

Henry Goldberg
Goldberg, Godies, Wiener & Wright
1229 Nineteenth St. NW
Washington, DC 20036
Counsel for Hewlett-Packard Company

Gerard J. Waldron
Mary Newcomer Williams
Covington & Burling
1201 Pennsylvania Ave. NW
Washington, DC 20004-2401
Counsel for Microsoft Corp.

Kurt A. Wimmer
Covington & Burling
1201 Pennsylvania Avenue NW
Washington, DC 20004-2401
Counsel for National Football League

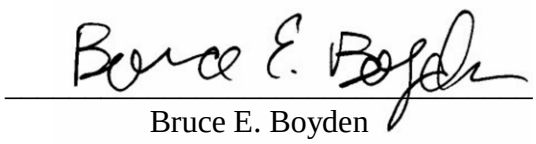
Lawrence R. Sidman
Sara W. Morris
Paul, Hastings, Janofsky & Walker LLP
1299 Pennsylvania Ave. NW, 10th Fl.
Washington, DC 20004
Counsel for Philips Electronics North America Corp. and Thomson

Nathan Mitchler
Mike Godwin
Public Knowledge
1875 Connecticut Ave. NW, Suite 650
Washington, DC 20009
Counsel for Public Knowledge

Laura H. Phillips
Drinker, Biddle & Reath LLP
1500 K Street NW, Suite 1100
Washington, DC 20005-1209
Counsel for RealNetworks, Inc.

Jennifer Coplan
Debevoise & Plimpton
919 Third Avenue
New York, NY 10022
Counsel for Sony Corp.

James M. Burger
Briana E. Thibeau
Dow, Lohnes & Albertson PLLC
1200 New Hampshire Ave. NW, Suite 800
Washington, DC 20036-6802
Counsel for TiVo Inc.



Bruce E. Boyden